	Application No.	Applicant(s)	
Notice of Allowability	09/975,410	VIALEN ET AL.	
	Examiner	Art Unit	
	John Pezzlo	2662	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 5 August 2005.*

2. ☒ The allowed claim(s) is/are *4-24 (renumbered 1-21 respectively).*

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☒ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

        Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 10/10/01, ≗...... *10/26/04*

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

JOHN PEZZLO
PRIMARY EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David E. Brown on 9 September 2005.

The claims have been amended as follows:

1.   Claim 12, line 1, changed "12" to -- 11 --.

2.   Claim 19, line 7, after "channels" deleted "," and inserted -- ; and transmitting information relating to the integrity output from one of said nodes to the other node, --.

3.   Claim 21, line 4, deleted "and".

4.   Claim 21, line 6, after "procedure" deleted "," and inserted -- ; and transmitting said integrity parameters from one of said nodes to the other node, --.

5.   Claim 21, line 7, deleted "said".

6.   Claim 22, line 9, after "identity," inserted -- wherein said information relating to the identity of the channel is combined with only one other input value. --.

7.   Claim 23, line 7, after "channels;" inserted -- means for transmitting information relating to the integrity output from one of said nodes to the other node; --.

8.   Claim 24, line 7, after "channels;" inserted -- wherein information relating to the integrity output is transmitted from one of said nodes to the other node, and --.

Allowable Subject Matter

Claims 4-24 are allowable over the prior art of record.

Reasons for Allowance

The following is an examiner's statement of reasons for allowance: Applicants have claimed the following uniquely distinct features in the instant invention, which are not found in the prior art, either singularly or in combination:

1.   Regarding claim 4 - A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of: calculating an integrity output, said integrity output being calculated from a plurality of input values, some of said input values being the same for said different channels, at least one of said input values being arranged to comprise information relating to the identity of said channels, each channel having a different identity and at least one of said input values are identical for said different channels, and transmitting information relating to the

integrity output from one of said nodes to the other, wherein said information relating to the identity of the channel is combined with only one other input value.

2.   Regarding claim 5 - A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of: calculating an integrity output, said integrity output being calculated from a plurality of input values, some of said input values being the same for said different channels, at least one of said input values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said input values are identical for said different channels, and transmitting information relating to the integrity output from one of said nodes to the other, wherein said information relating to the identity of the channel is combined with at least one other input value, and wherein said combined input value input comprises a first part allocated to the identity of the bearer and a second part allocated to the other information provided by said value.

3.   Regarding claim 7 - A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of: calculating an integrity output, said integrity output being calculated from a plurality of input values, some of said input values being the same for said different channels, at least one of said input values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said input values are identical for said different channels, and transmitting information relating to the integrity output from one of said nodes to the others wherein said information relating to the identity of the channel is combined with at least one other input value, and wherein said

information relating to the identity of the channel is combined with one or more of the following

values input to an algorithm: a fresh value, a count value, and integrity key, a direction value and

a message value.

4.   Regarding claim 19 - A method for carrying out an integrity check for an system

comprising a first node and a second node, a plurality of communication channels being

provided between said first node and said second node, said method comprising the step of

calculating an integrity output using a plurality of values, at least one of said values being

arranged to comprise information relating to the identity of said channel, each having a different

identity and at least one of said values being identical for said different channels, and

transmitting information relating to the integrity output from one of said nodes to the other node,

wherein said information relating to the identity of the channel is combined with only one other

input value.

5.   Regarding claim 20 - A method of communication between a first node and a second

node, a plurality of different channels being provided between said first and second node, said

method comprising the steps of: calculating an integrity output using a plurality of values, one of

said values being an integrity key, each of said channels having a different integrity key, and

transmitting information relating to the output of an integrity algorithm from one of said nodes to

the other, wherein said information relating to the identity of the channel is combined with only

one other input value.

6.   Regarding claim 21 - A method of communication between a first node and a second

node, a plurality of different channels being provided between said first and second node, said

method comprising: triggering an authentication procedure, calculating a desired number of

integrity parameters by the authentication procedure, and transmitting said integrity parameters

from one of said nodes to the other node, wherein information relating to the identity of the

channel is combined with only one other input value.

7.   Regarding claim 22 - A node, said node for use in a system comprising a said node and a

further node, a plurality of different channels being provided between said nodes, said node

comprising means for calculating an integrity output, said integrity output being calculated from

a plurality of values, at least one of said values being arranged to comprise information relating

to the identity of said values being arranged to comprise information relating to the identity of

said channel, each channel having a different identity and at least one of said values being

identical for said different channels, at least one of said values being arranged to comprise

information relating to the identity of said channel, each channel having a different identity,

wherein one of said nodes transmits information relating to the integrity output to the other node,

and wherein said information relating to the identity of the channel is combined with only one

other input value.

8.   Regarding claim 23 - A node, said node for use in a system comprising said node and a

further node, a plurality of different channels being provide between said nodes, said node

comprising means for calculating an integrity output, said integrity output being calculated from

a plurality of values, at least one of said values being arranged to comprise information relating

to the identity of said channel, each channel having a different identity and at least one of said

values being identical for said different channels, means for transmitting information relating to

the integrity output from one of said nodes to the other node, and means for comparing

information relating to the integrity output calculated by said node with a value calculated by the

further nodes wherein said information relating to the identity of the channel is combined with only one other input value.

9.   Regarding claim 24 - An algorithm for calculating an integrity output for use in a system comprising a node and a further node, a plurality of different channels being provided between said nodes, said algorithm comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, at least on of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity and at least one of said values being identical for said different channels, wherein information relating to the integrity output is transmitted from one of said nodes to the other node, and wherein said information relating to the identity of the channel is combined with at least one other input value.

The closest prior art, either singularly or in combination, fail to anticipate or render the above limitations obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Claims 4-24 being allowable, **Prosecution On The Merits Is Closed** in this application.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1.   Schneier et al. (US 5,970,143) discloses remote-auditing of computer generated outcomes, authenticated billing and access control, and software metering system using cryptographic and other protocols.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Pezzlo whose telephone number is (571) 272-3090. The examiner can normally be reached on Monday to Friday from 8:30 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou, can be reached on (571) 272-3088. The fax phone number for the organization where this application or proceeding is assigned is (571) 272-3090.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2600.

Any response to this action should be mailed to:

> Commissioner of Patents and Trademarks
>
> Washington, D.C.

or faxed to:

> (571) 272-3090

For informal or draft communications, please label "PROPOSED" or "DRAFT"

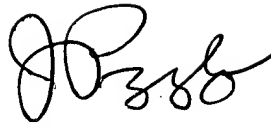Hand delivered responses should be brought to:

> Jefferson Building

2A15

500 Dulany Street

Alexandria, VA, 22313.

John Pezzlo

13 September 2005

JOHN PEZZLO
PRIMARY EXAMINER